Le Projet Pegasus : des fuites massives de données révèlent que le logiciel espion israélien de NSO Group est utilisé contre des militant·e·s, des journalistes et des dirigeant·e·s politiques partout dans le monde

Une grande enquête sur des fuites massives concernant 50 000 numéros de téléphone désignés comme cibles potentielles du logiciel espion de NSO Group révèle que ce logiciel a été utilisé pour favoriser des atteintes aux droits humains à grande échelle partout dans le monde. Parmi les personnes désignées comme des cibles potentielles figurent des dirigeant·e·s politiques, des militant·e·s et des journalistes, dont la famille de Jamal Khashoggi.

Le Projet Pegasus est une collaboration sans précédent menée par plus de 80 journalistes de 17 médias dans 10 pays et coordonnée par Forbidden Stories, une ONG basée à Paris travaillant dans le secteur des médias, avec le soutien technique d'Amnesty International, qui ont mené des analyses techniques de pointe visant à détecter des traces du logiciel espion Pegasus dans des téléphones portables.

« Le Projet Pegasus montre à quel point le logiciel espion de NSO Group est une arme de choix pour les gouvernements répressifs qui cherchent à réduire au silence les journalistes, à s'en prendre aux militant·e·s et à écraser l'opposition, mettant ainsi d'innombrables vies en péril », a déclaré Agnès Callamard, secrétaire générale d'Amnesty International.

« Ces révélations réduisent à néant toutes les affirmations de NSO Group selon lesquelles ces attaques sont rares et liées à une utilisation peu scrupuleuse de sa technologie. Bien que l'entreprise affirme que son logiciel espion est utilisé exclusivement à des fins légitimes d'enquêtes pénales et terroristes, il est clair que sa technologie favorise des atteintes systématiques. L'entreprise affiche une image de légitimité, tout en profitant d'atteintes généralisées aux droits humains. »

« Clairement, ses actions posent des questions plus importantes sur le manque général de régulation qui a créé un véritable Far West dans lequel les militant·e·s et les journalistes sont pris pour cible de façon abusive et généralisée. Tant que cette entreprise et ce secteur ne seront pas en mesure de prouver qu'ils sont capables de respecter les droits humains, il faut appliquer un moratoire immédiat sur l'exportation, la vente, le transfert et l'utilisation des technologies de surveillance. »

Dans une réponse écrite à Forbidden Stories et ses partenaires du secteur des médias, NSO Group a déclaré « nier fermement [...] les fausses accusations » de l'enquête. L'entreprise a déclaré que les informations du consortium étaient basées sur des « hypothèses erronées » et des « théories non corroborées » et a répété que l'entreprise menait une « mission vitale ». Une version plus longue de la réponse de NSO Group est disponible ici.

L'enquête

Au centre de cette enquête se trouve le logiciel espion de NSO Group qui, lorsqu'il est subrepticement installé dans le téléphone d'une personne, permet à l'auteur de l'attaque d'avoir entièrement accès au contenu de ce téléphone (SMS, courriels, activité sur Internet, micro, appareil photo, appels téléphoniques et contacts).

La semaine du 19 juillet 2021, des médias partenaires du Projet Pegasus – tels que *The Guardian*, *Le Monde*, le *Süddeutsche Zeitung* et *The Washington Post* – publieront une série d'articles détaillant comment des dirigeant·e·s mondiaux, des personnalités politiques, des défenseur·e·s des droits humains, des militant·e·s et des journalistes ont été choisis comme cibles potentielles de ce logiciel espion.

À partir des données divulguées et de leurs enquêtes, Forbidden Stories et ses partenaires du secteur des médias ont identifié des clients potentiels de NSO dans 11 pays : Arabie saoudite, Azerbaïdjan, Bahreïn, Émirats arabes unis, Hongrie, Inde, Kazakhstan, Mexique, Maroc, Rwanda et Togo.

L'entreprise NSO Group n'a pas pris les actions nécessaires pour mettre un terme à l'utilisation de ses outils aux fins de surveillance ciblée illégale de militant·e·s et de journalistes, alors qu'elle avait connaissance ou aurait sans doute dû avoir connaissance de cette utilisation abusive.

« NSO Group doit en premier lieu fermer immédiatement les systèmes de ses clients dès lors qu'il existe des preuves crédibles d'utilisation abusive – preuves que le Projet Pegasus fournit à la pelle », a déclaré Agnès Callamard.

La famille Khashoggi prise pour cible

L'enquête a également révélé de nouveaux éléments prouvant que des membres de la famille du journaliste saoudien Jamal Khashoggi avaient été pris pour cible par le logiciel Pegasus avant et après son assassinat à Istanbul le 2 octobre 2018 par des agents saoudiens, bien que NSO Group l'ait nié à maintes reprises.

Le Security Lab d'Amnesty International a établi que le logiciel espion Pegasus avait été installé avec succès sur le téléphone de la fiancée de Jamal Khashoggi, Hatice Cengiz, quatre jours seulement après l'assassinat du journaliste.

L'épouse de Jamal Khashoggi, Hanan Elatr, a elle aussi été prise pour cible à plusieurs reprises par le logiciel espion entre septembre 2017 et avril 2018, tout comme son fils, Abdullah, qui avait aussi été désigné comme cible potentielle, ainsi que d'autres membres de la famille en Arabie saoudite et aux Émirats arabes unis

Dans une déclaration, NSO Group a répondu aux allégations du Projet Pegasus que « sa technologie n'était en rien associée à l'assassinat haineux de Jamal Khashoggi ». L'entreprise a affirmé qu'elle avait « déjà enquêté sur cette affirmation, immédiatement après le crime » et que, « une fois encore, cette accusation était sans fondement ».

Des journalistes attaqués

L'enquête a identifié pour l'instant au moins 180 journalistes de 20 pays qui ont été désignés comme cibles potentielles du logiciel espion de NSO entre 2016 et juin 2021, notamment en Azerbaïdjan, en Hongrie, en Inde et au Maroc, des pays où la répression contre les médias indépendants s'est intensifiée.

Ces révélations montrent le tort que la surveillance illégale cause dans le monde réel.

- Au Mexique, le téléphone du journaliste Cecilio Pineda a été choisi comme cible quelques semaines seulement avant que celui-ci ne soit tué en 2017. Le Projet Pegasus a identifié au moins 25 journalistes mexicains ayant été désignés comme cibles en l'espace de deux ans. NSO Group a affirmé que bien que le téléphone de Cecilio Pineda ait été pris pour cible, les données recueillies de l'appareil n'ont pas contribué à sa mort.
- Pegasus a été utilisé en Azerbaïdjan, un pays où il ne reste plus qu'une poignée de médias indépendants. Selon l'enquête, 40 journalistes azerbaïdjanais figuraient parmi les cibles potentielles visées. Le Security Lab d'Amnesty International a ainsi découvert que le téléphone de Sevinc Vaqifqizi, journaliste freelance pour le média indépendant Meydan TV, avait été infecté pendant deux ans jusqu'en mai 2021.
- En Inde, au moins 40 journalistes de presque tous les grands médias du pays ont été désignés comme cibles entre 2017 et 2021. Les analyses techniques ont révélé que les téléphones de Siddharth Varadarajan et de M. K. Venu, cofondateurs du média en ligne indépendant The Wire, avaient été infectés par le logiciel espion Pegasus pas plus tard qu'en juin 2021.
- L'enquête a également identifié parmi les cibles potentielles des journalistes travaillant pour de grands médias internationaux, comme Associated Press, CNN, le *New York Times* et Reuters. Au rang des journalistes les plus connus figurait Roula Khalaf, rédactrice en chef du *Financial Times*.

« Le nombre de journalistes identifiés comme cibles montre clairement que Pegasus est utilisé comme outil pour intimider les médias qui critiquent le pouvoir. Il s'agit pour les autorités de contrôler le discours public, de résister à toute surveillance et de réprimer les voix dissidentes », a déclaré Agnès Callamard.

« Ces révélations doivent être des catalyseurs de changement. Le secteur de la surveillance ne doit plus bénéficier d'un tel laissez-faire de la part de gouvernements qui ont des intérêts particuliers à utiliser cette technologie pour commettre des atteintes aux droits humains. »

Révélation de l'infrastructure de Pegasus

Amnesty International publie aujourd'hui les détails techniques complets des analyses techniques réalisées par son Security Lab dans le cadre du Projet Pegasus.

Le rapport de méthodologie du Security Lab montre l'évolution des attaques menées au moyen du logiciel espion Pegasus depuis 2018, et donne des détails sur l'infrastructure du logiciel espion, dont plus de 700 domaines liés à Pegasus.

« NSO affirme que son logiciel espion est indétectable et utilisé uniquement à des fins légitimes d'enquêtes pénales. Nous avons maintenant apporté des preuves irréfutables que c'est absolument faux », a déclaré Etienne Maynier, expert des nouvelles technologies à Amnesty Tech.

Rien ne laisse penser que les clients de NSO n'ont pas également utilisé Pegasus dans le

cadre d'enquêtes pénales ou terroristes, et le consortium Forbidden Stories a également trouvé de nombreuses données appartenant à des criminels présumés.

« Il faut mettre un terme aux atteintes généralisées aux droits humains que Pegasus favorise. Nous espérons que les preuves accablantes publiées la semaine prochaine amèneront les gouvernements à réformer le secteur de la surveillance, qui est actuellement hors de contrôle. » a déclaré Etienne Maynier.

En réponse à une demande de commentaire formulée par des organisations médiatiques impliquées dans le Projet Pegasus, NSO Group a déclaré « nier fermement » les accusations, affirmant qu'elles sont « pour beaucoup des théories non corroborées, qui jettent de sérieux doutes sur la crédibilité de vos sources, ainsi que sur le cœur de votre enquête ». NSO Group n'a ni confirmé ni démenti les informations sur les gouvernements faisant partie de ses clients, bien que l'entreprise ait déclaré que le Projet Pegasus avait fait des « hypothèses incorrectes » à cet égard. Tout en niant les affirmations, NSO Group a déclaré que l'entreprise « continuerait d'enquêter sur toutes les allégations crédibles d'utilisation abusive et prendrait les mesures adaptées en fonction des résultats de ces enquêtes. »

FIN